# Prawne aspekty wykorzystania technologii *cloud computing* w sektorze opieki zdrowotnej

*Katarzyna Biczysko-Pudełko*[1]

Celem niniejszego opracowania jest próba poszukiwania odpowiedzi na pytanie o prawne implikacje wykorzystywania technologii *cloud computing* (chmury obliczeniowej) w sektorze opieki zdrowotnej, a ściślej możliwości przetwarzania danych dotyczących zdrowia w ramach elektronicznej dokumentacji medycznej funkcjonującej w takich systemach informatycznych jak chmura obliczeniowa. Stąd też głównym tłem rozważań będą przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) z 27.4.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[2], a także – w mniejszym jednak zakresie – przepisy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[3], i przyjęte na jej podstawie przepisy prawa polskiego.

## Uwagi wstępne

Chmura obliczeniowa (*cloud computing*), będąca właściwie synonimem przetwarzania danych, w praktyce sprowadza się do wszechobecnego, wygodnego i możliwego na żądanie dostępu za pośrednictwem sieci do dzielonych zasobów obliczeniowych (tj. sieć, serwery, pamięć masowa, aplikacje i usługi), które mogą być szybko zapewnione i uwolnione przy minimalnym zarządzaniu lub ingerencji dostawcy[4]. Przedmiotowa technologia, niegdyś określana mianem „technologii jutra", z roku na rok zyskuje coraz szersze grono użytkowników wykorzystujących jej możliwości w często zupełnie różnych od siebie celach, tj. od poczty elektronicznej wykorzystywanej *stricte* na potrzeby korespondencji prywatnej począwszy, poprzez portale społecznościowe, różnego rodzaju pakiety biurowe, a na zaawansowanych środowiskach programistycznych skończywszy. Powyższy trend nie ominął także sektora opieki zdrowotnej, w ramach funkcjonowania którego technologia ta zdaje się zyskiwać na znaczeniu i popularności. Każdego dnia w rzeczonym sektorze dochodzi do przetwarzania setek tysięcy danych, przy czym procesy te – w mojej ocenie – co do zasady odbywają się w dwóch obszarach, tj.:

– obszarze organizacyjnym, w ramach którego instaluje się system informatyczny, w praktyce pozwalający na zastąpienie dotychczasowych papierowych nośników danych o pacjencie nośnikami elektronicznymi i sprowadzający się m.in. do tworzenia elektronicznej dokumentacji medycznej;
– obszarze klinicznym – sprowadzającym się do wykorzystania usług chmury obliczeniowej do świadczenie usług opieki zdrowotnej (tj. diagnozowania, leczenia, profilaktyki chorób, a także urazów, jak również badań i ich oceny) w sytuacjach, w których pracownicy systemu opieki zdrowotnej i pacjenci znajdują się w różnych miejscach – tj. obszar telemedycyny.

Mając więc na uwadze powyższe, a także wzajemną implikację pomiędzy koniecznością zapewnienia pacjentom poufności i bezpieczeństwa ich danych – z jednej strony zwłaszcza z uwagi na potencjalne konsekwencje ich naruszenia[5], oraz z drugiej strony proces stale postępującej informatyzacji[6] sek-

[1] Uniwersytet Opolski.

[2] Dz.Urz. UE L Nr 119, s. 1, dalej jako: RODO.

[3] Dz.Urz. UE L Nr 194, s. 2; dalej jako: dyrektywa NIS.

[4] *P. Mell*, *T. Grance*, The NIST Definition of Cloud Computing: Recommendations of National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, MD September 2011, s. 2. Zob. także Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie wykorzystania potencjału chmury obliczeniowej w Europie, COM (2012) 529 final, s. 2; *J. Byrski*, *A. Wachowska*, Cloud computing w działalności instytucji płatniczej, Monitor Prawa Bankowego 2012, Nr 9, s. 59; *D. Szostek*, Nowe ujęcie dokumentu w polskim prawie prywatnym ze szczególnym uwzględnieniem dokumentu w postaci elektronicznej, Warszawa 2012, s. 56–57.

[5] Odnosząc się do konsekwencji naruszenia danych osobowych przetwarzanych w sektorze ochrony zdrowia, wskazać należy, iż sektor ten słusznie oceniany jest jako krytyczny. Dowodzi tego fakt coraz częstszych ataków hakerskich, których to celami stają się m.in. szpitale czy placówki medyczne. Tytułem przykładu wskazać można chociażby na ataki, jakie nastąpiły w Wielkiej Brytanii, gdzie w 2017 r. nieznani hakerzy dokonali masowego ataku na szpitale należące do National Health Service, atakując m.in. komputery podmiotów leczniczych przez tzw. ransomware, czego konsekwencją była chociażby konieczność przeniesienia pacjentów do innych placówek i odwołanie części zabiegów. Co więcej, podnieść należy, iż np. w Stanach Zjednoczonych co dziesiąty podmiot leczniczy każdego dnia doświadcza próby włamania. Zob. więcej: *P. Najbuk*, *P. Kaźmierczak*, *W. Dziomdziora*, *P. Marczuk*, Cyberbezpieczeństwo w sektorze ochrony zdrowia, Warszawa 2017, s. 5, https://portal.dzp.pl/files/shares/Cyberbezpiecze%C5%84stwo%20w%20sektorze%20zdrowia% 20 raport% 20 DZP.pdf (dostęp z 20.12.2017 r.).

[6] Pojęcie informatyzacji jest pojęciem szerszym od określenia komputeryzacji i polega ono m.in. na racjonalnym wykorzystaniu uprzednio wprowadzonych już danych w postaci elektronicznej do systemów teleinformatycznych w możliwie największym dopuszczalnym zakresie, także przez systemy teleinformatyczne innych podmiotów, Zob. *S. Kotecka*, E-Government & E-Justice, [w:] *A. Burdziak*, *Ł. Cieślak*, *Ł. Goździaszek*, *S. Kotecka*, *P. Pęcherzewski*, *P. Rodziewicz*, *A. Zalesińska* (red.), Technologia informacyjna dla prawników (dokument elektroniczny), Wrocław 2011, s. 52. Na temat pojęcia informatyzacji i komputeryzacji. Szerzej zob. *J. Gołaczyński*, *S. Kostecka*, Klikając Temid@, Prawo Mediów Elektronicznych 2011/3, Warszawa 2011, s. 11–15.

tora opieki zdrowotnej, jako istotna, ale jednocześnie ciekawa, jawi się analiza dotycząca poszukiwania odpowiedzi na pytanie o prawne implikacje wykorzystywania interesującej nas technologii *cloud computing* właśnie w sektorze opieki zdrowotnej, przy czym zakres przedmiotowej analizy zostanie ograniczony tylko do wspomnianego wyżej obszaru organizacyjnego z jednoczesnym uwzględnieniem przepisów RODO. Powyższe znajduje swoje uzasadnienie chociażby w twierdzeniu, że o ile sam fakt stale rosnącej już przecież od co najmniej kilkunastu lat komputeryzacji[7] podmiotów świadczących usługi w systemie ochrony zdrowia zdawał się nie rodzić aż tak daleko idących konsekwencji dla ochrony danych osobowych, o tyle już zmiana podstawowego medycznego nośnika danych, tj. dokumentów w formie papierowej, na dane w postaci elektronicznej, a następnie ich przetwarzanie właśnie za pomocą chmury obliczeniowej z całą pewnością jest o wiele bardziej złożone i to nie tylko technologicznie, ale także prawnie, a to z następujących względów.

Przede wszystkim wymaga ono uwzględnienia kilku norm prawnych obowiązujących nie tylko w przestrzeni prawa ochrony danych osobowych, ale także tzw. regulacji sektorowych skupionych zarówno w wielu ustawach, jak i w aktach wykonawczych[8], które co do zasady – jak wskazują *A. Romaszewski* i *W. Trąbka*[9] – sklasyfikować można do następujących grup:

a) regulacje dotyczące kwestii elektronicznej dokumentacji medycznej, czego w szczególności[10] dotyczyć będzie ustawa z 28.4.2011 r. o systemie informacji w ochronie zdrowia[11];
b) regulacje dotyczące zasad postępowania z danymi o charakterze osobowym gromadzonymi przez podmioty udzielające świadczeń medycznych w procesie realizowania swoich zadań, które to dane mogą także zostać, w myśl art. 24 ust. 5 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta powierzone przez podmiot udzielający świadczeń zdrowotnych do dalszego przetwarzania na podstawie umowy o powierzenie przetwarzania danych osobowych, o której to mowa w art. 28 RODO;
c) regulacje dotyczące ochrony baz danych[12] ze szczególnym uwzględnieniem baz zawierających dane o stanie zdrowia, prowadzonych na zasadzie obowiązku przez wszystkie podmioty zobowiązane do tego ustawą o systemie informacji w ochronie zdrowia;
d) wiele przepisów zawartych w ustawie o systemie informacji w ochronie zdrowia oraz ustawie z 17.2.2005 r. o informatyzacji podmiotów publicznych realizujących zadania publiczne[13] wraz z rozporządzeniami wykonawczymi;
e) regulacje zapewniające odpowiedni poziom integralności sieci, usług oraz przekazu komunikatów przez operatorów (dostawców usług) świadczących usługi telekomunikacyjne[14].

Dodatkowo na złożoność problematyki przetwarzania danych dotyczących zdrowia wpływ ma także liczba podmiotów, które do przedmiotowego przetwarzania są uprawnione, tj.: pacjent, którego dane są przetwarzane, podmiot, który udziela świadczeń zdrowotnych, podmiot upoważniony na podstawie przepisów prawa i w zakresie określonym przepisami (np. NFZ[15]), czy też podmioty, które dostarczają zasoby, infrastrukturę lub inne usługi w chmurze, oraz podmioty odpowiedzialne za transmisje danych w sieciach teleinformatycznych[16]. Co znamienne, każda z wyżej wymienionych grup podlega innym regulacjom prawnym, to zaś prowadzi także do odmiennego kształtowania nie tylko ich praw i obowiązków, ale też ich odpowiedzialności[17].

---

[7] Pojęcie komputeryzacji należy rozumieć jako stosowanie komputerów w różnego rodzaju organizacjach i wprowadzanie metod przetwarzania danych przy ich użyciu. W ramach komputeryzacji zastępuje się np. własnoręcznie uzupełniane formularze – formularzami elektronicznymi wypełnianymi za pomocą edytorów tekstu, archiwa dokumentów sporządzonych na papierze – bazami dokumentów elektronicznych, wprowadza się pocztę elektroniczną lub komunikator internetowy jako prawnie relewantny środek komunikacji pomiędzy pracownikami danego podmiotu a klientami. Zmienia się jednak jedynie narzędzie pracy – z długopisu na klawiaturę i myszkę komputerową oraz monitor. Tworzone bazy dokumentów elektronicznych i danych zawartych w tych dokumentach nie są udostępniane nawet innym komórkom organizacyjnym danej jednostki, nie mówiąc o udostępnianiu tychże baz innym podmiotom. Pojęcie komputeryzacji jest pojęciem węższym w stosunku do określenia informatyzacji. Zob. *S. Kotecka*, E-Government & E-Justice..., s. 52.

[8] Np. rozporządzenie Prezesa Rady Ministrów z 14.9.2011 r. w sprawie sporządzania pism w formie dokumentów elektronicznych, doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 r. poz. 180); rozporządzenie Rady Ministrów z 12.4.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r. poz. 2247 ze zm.); rozporządzenie Ministra Zdrowia z 25.3.2013 r. w sprawie klasyfikacji danych i systemu kodów w Systemie Informacji Medycznej (Dz.U. poz. 473 ze zm.); rozporządzenie Ministra Zdrowia z 6.4.2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. poz. 666), dalej jako: DokMedR.

[9] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych, Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie 2014, Nr 33, s. 37–38.

[10] Ponadto można wskazać jeszcze na następujące akty prawne: ustawę z 15.4.2011 r. o działalności leczniczej (t.j. Dz.U. z 2020 r. poz. 295 ze zm.; dalej jako: DziałLeczU), ustawę z 6.11.2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (t.j. Dz.U. z 2020 r. poz. 849 ze zm.; dalej jako: PrPacjentU); ustawę z 5.12.1996 r. o zawodach lekarza i lekarza dentysty (t.j. Dz.U. z 2020 r. poz. 514 ze zm.).

[11] T.j. Dz.U. z 2020 r. poz. 702 ze zm., dalej jako: SysInfZdrowU.

[12] Ustawa z 27.7.2001 r. o ochronie baz danych (Dz.U. Nr 128, poz. 1402 ze zm.).

[13] T.j. Dz.U. z 2017 r. poz. 570 ze zm.

[14] Ustawa z 16.7.2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907 ze zm.).

[15] Narodowy Fundusz Zdrowia jest państwową jednostką organizacyjną działającą na podstawie ustawy z 27.8.2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (t.j. Dz.U. z 2020 r. poz. 1398 ze zm.; dalej jako: ŚwŚrodPubU) i w ramach polskiego systemu opieki zdrowotnej pełni funkcję płatnika.

[16] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych..., s. 38.

[17] *Ibidem*.

## Kazus elektronicznej dokumentacji medycznej

Pomimo wskazanych wcześniej okoliczności obecnie podejmowane są realne działania mające na celu realizację w ramach systemu ochrony zdrowia bardzo dużych projektów właśnie na bazie technologii *cloud computing*[18], czego dobrym przykładem zdaje się być kazus elektronicznej dokumentacji medycznej. I jakkolwiek przepisy wprowadzające elektroniczną dokumentację medyczną jako standardową i powszechnie obowiązującą były już wielokrotnie nowelizowane[19], a ostateczny termin obowiązku posługiwania się tego typu dokumentacją zmieniany, niemniej jednak w praktyce systemu opieki zdrowotnej „papierowy" dokument przechodzi wolno do historii i zauważalne jest świadczenie przez wiele podmiotów usług medycznych przy wsparciu modelu elektronicznej dokumentacji medycznej, w tym także poza miejscem świadczenia usług zdrowotnych i przy wykorzystaniu technologii *cloud computing*[20].

Dostrzegając powyższe, nie sposób więc nie odnieść się do przedmiotowego zjawiska, co jednakże wcześniej warto poprzedzić kilkoma uwagami natury ogólnej.

W literaturze przedmiotu słusznie zauważa się, że w praktyce funkcjonowania rynku usług medycznych dane i informacje, które już są lub mają być w przyszłości przetwarzane w ramach chmury obliczeniowej, występują obecnie w różnych formach zarówno pod względem nazewnictwa, zawartości merytorycznej, jak i organizacyjnej[21].

Doskonale obrazują to chociażby przepisy ustawy o systemie informacji w ochronie zdrowia, w ramach której można, poza wspomnianą już elektroniczną dokumentacją medyczną, napotkać jeszcze kategorie takich pojęć jak: „dane"[22], „jednostkowe dane medyczne", „dokument elektroniczny"[23], „bazy danych"[24] czy „rejestr medyczny"[25]. Wspólnym mianownikiem dla wszystkich tych danych jest natomiast to, że funkcjonują w ramach tzw. systemu informacji w ochronie zdrowia, a więc systemu, w którym przetwarzane są dane niezbędne do prowadzenia polityki zdrowotnej państwa, podnoszenia jakości i dostępności świadczeń opieki zdrowotnej oraz finansowania zadań z zakresu ochrony zdrowia (art. 1 ust. 1 SysInfZdrowU) i który to obejmuje bazy danych tworzone przez podmioty obowiązane do ich prowadzenia, zawierające dane o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej, usługodawcach i pracownikach medycznych, usługobiorcach (art. 3 ust. 1 SysInfZdrowU) oraz które to bazy danych funkcjonują w ramach systemu informacji medycznej (SIM), dziedzinowych systemów teleinformatycznych, o których mowa w art. 5 ust. 1 pkt 2 SysInfZdrowU, oraz rejestrów medycznych (art. 5 ust. 1 SysInfZdrowU).

Z całego spektrum wskazanych powyżej danych to jednak elektroniczna dokumentacja medyczna będzie podstawowym nośnikiem danych i informacji o stanie zdrowia i to właśnie w ramach elektronicznej dokumentacji medycznej dochodzić będzie do przetwarzania zwłaszcza jednej ze szczególnych kategorii danych osobowych, o których mowa na gruncie art. 4 pkt 15 RODO, a więc do przetwarzania danych osobowych o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniających informacje o jej stanie zdrowia („dane dotyczące zdrowia").

Ustawodawca polski w ramach przepisów ustawy o systemie informacji w ochronie zdrowia zaproponował, by pod pojęciem elektronicznej dokumentacji medycznej rozumieć dokumenty wytworzone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym, podpisem osobistym albo z wykorzystaniem sposobu potwierdzania pochodzenia oraz integralności danych dostępnego w systemie teleinformatycznym udostępnionym bezpłatnie przez ZUS:

a) recepty,
b) określone w przepisach wydanych na podstawie art. 13a,
c) skierowania określone w przepisach wydanych na podstawie art. 59aa ust. 2 ŚwŚrodPubU.

---

[18] *Ibidem*.

[19] Zgodnie z pierwotnym brzmieniem ustawy o systemie informacji w ochronie zdrowia, wszelka dokumentacja medyczna wytworzona po 31.7.2014 r. miała być prowadzona w wersji elektronicznej. Niemniej jednak na skutek nowelizacji dokonanej ustawą z 26.6.2014 r. o zmianie ustawy o systemie informacji w ochronie zdrowia (Dz.U. poz. 998) wprowadzono przepis, zgodnie z którym do 31.7.2017 r. dokumentacja medyczna może być prowadzona w wersji papierowej lub elektronicznej. Następnie mocą ustawy z 9.10.2015 r. termin wprowadzenia elektronicznej dokumentacji medycznej przesunięto do 31.12.2017 r. (Dz.U. poz. 1991). Wreszcie według stanu prawnego obowiązującego w momencie tworzenia niniejszego opracowania ostatecznie obowiązek prowadzenia jej w wersji elektronicznej istnieć będzie od 1.1.2019 r. (Dz.U. z 2017 r. poz. 1845), przy czym wskazać należy, iż ustawodawca dokonał rozróżnienia terminu dla elektronicznej dokumentacji medycznej, recept elektronicznych (tj. od 1.1.2020 r.) i skierowań w postaci elektronicznej (od 1.1.2021 r.).

[20] *A. Romaszewski*, *W. Trąbka*, *M. Kielar*, *K. Gajda*, Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych, Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie 2017, Nr 44, s. 14.

[21] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych..., s. 42.

[22] Pod pojęciem tym, w świetle art. 2 pkt 4 SysInfZdrowU, rozumieć należy litery, wyrazy, cyfry, teksty, liczby, znaki, symbole, obrazy, kombinacje liter, cyfr, liczb, symboli i znaków, zebrane w zbiory o określonej strukturze, dostępne według określonych kryteriów, w tym dane osobowe.

[23] Przez sformułowanie dokument elektroniczny na gruncie ustawy o systemie informacji w ochronie zdrowia rozumieć należy dokument elektroniczny, o którym mowa w art. 3 pkt 2 ustawy z 17.2.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2020 r. poz. 346 ze zm.).

[24] Bazy danych, zgodnie z ustawą o systemie informacji w ochronie zdrowia, zawierają dane o udzielonych, udzielanych i planowanych świadczeniach opieki zdrowotnej; usługodawcach i pracownikach medycznych; usługobiorcach. Podmioty zobowiązane do ich prowadzenia wskazane zostały w art. 3 ust. 2 SysInfZdrowU.

[25] Zgodnie z art. 2 pkt 12 SysInfZdrowU rejestr medyczny to tworzony zgodnie z prawem rejestr, ewidencja, lista, spis albo inny uporządkowany zbiór danych osobowych, jednostkowych danych medycznych lub danych niebędących danymi osobowymi, służący do realizacji zadań publicznych, prowadzony przez podmiot funkcjonujący w systemie ochrony zdrowia.

Doprecyzowując powyższe, już na gruncie rozporządzenia w sprawie dokumentacji medycznej, ustawodawca wskazał, iż dokumentacja medyczna może być prowadzona w postaci papierowej, jeżeli przepis rozporządzenia tak stanowi lub warunki organizacyjno-techniczne uniemożliwiają prowadzenie dokumentacji w postaci elektronicznej (§ 1 DokMedR) i zasadniczo wyróżnić można dwa podstawowe jej rodzaje, tj. dokumentację indywidualną dotyczącą poszczególnych pacjentów korzystających ze świadczeń zdrowotnych oraz dokumentację zbiorczą odnoszącą się do ogółu pacjentów lub poszczególnych grup pacjentów korzystających ze świadczeń zdrowotnych (§ 2 DokMedR).

Co więcej, w ramach indywidualnej dokumentacji medycznej ustawodawca zdecydował się wyróżnić jeszcze tę przeznaczoną na potrzeby podmiotu udzielającego świadczeń zdrowotnych (tj. dokumentację indywidualną wewnętrzną) oraz tę przeznaczoną na potrzeby pacjenta korzystającego ze świadczeń zdrowotnych (tj. dokumentację indywidualną zewnętrzną). I to właśnie obie ze wskazanych powyżej kategorii dokumentacji indywidualnej będą z punktu widzenia przedmiotowej analizy mieć fundamentalne znaczenie. W zakresie pierwszej z nich mieścić będzie się w szczególności historia zdrowia i choroby, historia choroby, karta noworodka, karta indywidualnej opieki pielęgniarskiej, karta indywidualnej opieki prowadzonej przez położną, karta wizyty patronażowej itd. (§ 2 pkt 3 DokMedR). Z kolei indywidualna dokumentacja zewnętrzna dotyczyć będzie w szczególności skierowania do szpitala lub innego podmiotu na badania diagnostyczne, konsultacji lub leczenia, karty przebiegu ciąży, książeczki zdrowia dziecka, karty informacyjnej z leczenia szpitalnego czy też pisemnej informacji lekarza leczącego pacjenta w poradni specjalistycznej dla kierującego lekarza ubezpieczenia zdrowotnego lub felczera ubezpieczenia zdrowotnego oraz lekarza podstawowej opieki zdrowotnej o rozpoznaniu, sposobie leczenia, rokowaniu, ordynowanych lekach, środkach specjalnego przeznaczenia żywieniowego i wyrobach medycznych czy wreszcie też opinii lekarskiej (§ 2 pkt 4 DokMedR). Jednoznacznie więc – biorąc pod uwagę przytoczoną wcześniej definicję danych dotyczących zdrowia obowiązującą na gruncie RODO, wskazać należy, iż tego typu dane będą zawierać się właśnie w ramach indywidualnej dokumentacji medycznej i tym samym więc szerzej w ramach całej dokumentacji medycznej.

Powyższe prowadzi do wniosku, że elektroniczna dokumentacja medyczna będzie podstawowym nośnikiem danych i informacji o stanie zdrowia pacjenta[26], a warunkiem *sine quo non* do skorzystania z owej elektronicznej dokumentacji medycznej jest funkcjonowanie dedykowanego systemu teleinformatycznego[27].

W warunkach polskiej służby zdrowia, zgodnie z ustawą o systemie informacji w ochronie zdrowia, rolę owego dedykowanego systemu teleinformatycznego odgrywa tzw. SIM, tj. system informacji medycznej[28]. Zgodnie z art. 10 ust. 1 SysInfZdrowU, SIM jest systemem teleinformatycznym służącym przetwarzaniu danych dotyczących udzielonych, udzielanych i planowanych świadczeń opieki zdrowotnej udostępnianych przez systemy teleinformatyczne usługodawców[29]. W powiązaniu z danymi, o których mowa w ust. 1 art. 10 SysInfZdrowU, w SIM przetwarzane i udostępniane w postaci elektronicznej są m.in. dane osobowe i jednostkowe dane medyczne o usługobiorcach[30], dane o usługodawcach, dane o pracownikach medycznych, dane o płatnikach, o których mowa w art. 2 pkt 9 lit. a, oraz kilka innych danych wskazanych w art. 10 ust. 2 SysInfZdrowU. Ponadto, w myśl art. 11. ust. 3, usługodawca zamieszcza w SIM dane umożliwiające pobieranie danych zawartych w elektronicznej dokumentacji medycznej przez innego usługodawcę lub pobieranie dokumentów elektronicznych niezbędnych do prowadzenia diagnostyki, zapewnienia ciągłości leczenia. Szczegółowo katalog tychże danych określony został w art. 11 ust. 4 SysInfZdrowU i obejmuje on:

1) dane usługodawcy;
2) dane usługobiorcy;
3) dane identyfikujące świadczenie zdrowotne;
4) dane miejsca udzielenia świadczenia zdrowotnego;
5) dane pracownika medycznego udzielającego świadczenia zdrowotnego;
6) dane dotyczące dokumentacji medycznej wytworzonej w związku z udzielonym świadczeniem zdrowotnym;
7) inne dane pozwalające na identyfikację zdarzenia medycznego.

Jak wynika więc z powyższego, katalog danych, które usługodawca umieszcza w SIM, jest szeroki i z całą pewnością obejmuje on swoim zakresem również dane dotyczące zdrowia, stąd też konsekwencje naruszeń bezpieczeństwa tychże danych są potencjalnie znaczące i daleko idące.

Z tego względu nie może dziwić fakt nałożenia na podmioty udzielające świadczeń zdrowotnych wielu obowiązków i to nie tylko mocą przepisów z zakresu prawa ochrony danych, ale również regulacji sektorowych, jak np. normy rozporządzenia w sprawie dokumentacji medycznej. Te ostatnie zobowiązują podmioty udzielające świadczeń zdrowotnych do spełnienia wielu wymagań co do warunków prowadzenia

[26] *A. Romaszewski*, *W. Trąbka*, Aspekty prawne przetwarzania danych medycznych w chmurach obliczeniowych..., s. 42.

[27] *A. Klich*, Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej, Ekonomiczne Problemy Usług, 2017 (126), Nr 1, t. 2, Szczecin 2017, s. 355.

[28] Dalej jako: SIM.

[29] Zgodnie z art. 2 SysInfZdrowU pod pojęciem usługodawcy należy rozumieć świadczeniodawcę w rozumieniu art. 5 pkt 41 ŚwŚrodPubU, oraz aptekę ogólnodostępną i punkt apteczny.

[30] Usługobiorcą – w myśl art. 2 SysInfZdrowU – jest osoba fizyczna korzystająca lub uprawniona do korzystania ze świadczeń opieki zdrowotnej, w tym świadczeniobiorca w rozumieniu art. 2 ust. 1 ŚwŚrodPubU oraz osoba, o której mowa w art. 2 ust. 2 i art. 13 tej ustawy.

dokumentacji medycznej w postaci elektronicznej, warunków jej zabezpieczenia[31], a także warunków, jakie musi spełnić sam system teleinformatyczny, w ramach którego dochodzi do umieszczania elektronicznej dokumentacji medycznej[32].

Powyższy stan rzeczy sprawia, że znaczna część podmiotów udzielających świadczenia zdrowotne decyduje się na skorzystanie z możliwości, jaką daje art. 24 PrPacjentU, a mianowicie outsourcingu procesów przetwarzania danych medycznych na rzecz zewnętrznych podmiotów, w tym także w ramach usług *cloud computing*. Oczywiście w przedmiotowej sytuacji taki podmiot udzielający świadczeń zdrowotnych będzie zobligowany do spełnienia wielu innych obowiązków, które nakładają na niego, jako administratora tychże danych, przepisy RODO, tj. chociażby ustalenia, czy dany dostawca usług w chmurze obliczeniowej daje rękojmię zapewnienia odpowiedniego poziomu ochrony powierzonych mu danych osobowych, a sama realizacja tej umowy nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej. Jednocześnie jednak podmiot, któremu powierzono przetwarzanie danych osobowych, obowiązany jest do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją tej umowy, a związanie przedmiotową tajemnicą nie ustaje nawet po śmierci pacjenta (art. 24 ust. 6 PrPacjetU), a także innych obowiązków, które wynikają już wprost z przepisów RODO, jak np. związanych z prawidłową realizacją umowy związanych m.in. ze wsparciem administratora w wywiązywaniu się z obowiązku odpowiadania na żądania osób, których dane są przetwarzane, czy zapewnieniem odpowiednich środków technicznych i organizacyjnych ochrony powierzonych danych (art. 28 ust. 3 RODO). Ponadto, dostawca usług *cloud computing* powinien powstrzymać się od przekazywania danych do przetwarzania innym podmiotom bez uprzedniego uzyskania szczegółowej lub ogólnej pisemnej zgody administratora w tym zakresie (art. 28 ust. 2 RODO)[33]. W przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, który powierzył przetwarzanie danych osobowych.

## Technologia *cloud computing* w świetle przepisów dyrektywy NIS

Odnosząc się do tematu korzystania przez sektor opieki zdrowotnej z technologii *cloud computing*, nie można jednocześnie pominąć przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.7.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[34], i przyjętych na jej podstawie przepisów prawa polskiego.

W dużym uogólnieniu przepisy dyrektywy NIS nakładają na państwa członkowskie obowiązek zidentyfikowania do 9.11.2018 r. tzw. operatorów kluczowych (mających jednostkę organizacyjną na terytorium ich państwa – art. 5 ust. 1 dyrektywy NIS) oraz określenia obowiązków związanych z zapewnieniem bezpieczeństwa cybernetycznego, jakie owe podmioty muszą spełnić. Dyrektywa NIS jako operatorów usług kluczowych kwalifikuje podmiot publiczny lub prywatny należący do jednego z następujących sektorów, tj. energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję, infrastruktury cyfrowej, i który to podmiot świadczy usługę mającą kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, świadczenie tej usługi zależy od sieci i systemów informatycznych oraz incydent miałby istotny skutek zakłócający dla świadczenia tej usługi (art. 4 pkt 4 dyrektywy NIS). Innymi słowy, jak wynika z powyższego, dostawcy usług dla ochrony zdrowia, w tym ci obsługujący rozwiązania chmurowe, będą musieli być wskazani przez państwo[35].

Do polskiego systemu prawnego dyrektywa NIS została implementowana przepisami ustawy z 5.7.2018 r. o krajowym systemie cyberbezpieczeństwa[36], której to przepisy obowiązują od 28.8.2018 r., przy czym wskazać należy, iż zgodnie z samą dyrektywą NIS państwa członkowskie zobowiązane zostały do 9.5.2018 r. przyjąć i opublikować przepisy ustawo-

[31] Dokumentację prowadzoną w postaci elektronicznej – w myśl § 1 pkt 4 DokMedR uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki: 1) jest zapewniona jej dostępność wyłącznie dla osób uprawnionych, o których mowa w art. 24 ust. 2 i art. 26 PrPacjentU oraz innych przepisach prawa powszechnie obowiązującego; 2) są zastosowane metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.

[32] Zgodnie z pkt 5 § 1 DokMedR zabezpieczenie dokumentacji wymaga w szczególności: 1) systematycznego szacowania ryzyka zagrożeń oraz zarządzania tym ryzykiem; 2) opracowania i stosowania udokumentowanych procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania; 3) stosowania środków bezpieczeństwa adekwatnych do zagrożeń, uwzględniających najnowszy stan wiedzy; 4) dbałości o aktualizację oprogramowania; 5) bieżącego kontrolowania funkcjonowania organizacyjnych i techniczno-informatycznych sposobów zabezpieczenia, a także okresowego dokonywania oceny skuteczności tych sposobów; 6) przygotowania i realizacji planów przechowywania dokumentacji w długim czasie, w tym jej przenoszenia na informatyczne nośniki danych i do nowych formatów danych, jeżeli tego wymaga zapewnienie ciągłości dostępu do dokumentacji.

[33] Zob. więcej na temat obowiązków dostawcy usług *cloud computing* jako przetwarzającego dane: *P. Litwiński*, *P. Barta*, *M. Kawecki*, [w:] *P. Litwiński* (red.), Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz, Warszawa 2018, s. 441 i n.

[34] Dz.Urz. UE L Nr 194, s. 2; dalej jako: dyrektywa NIS.

[35] *A. Romaszewski*, *W. Trąbka*, *M. Kielar*, *K. Gajda*, Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych..., s. 18.

[36] T.j. Dz.U. z 2020 r. poz. 1369 ze zm.; dalej jako: KrajSysCyberU.

we, wykonawcze i administracyjne[37] niezbędne do wykonania tejże dyrektywy (art. 25 ust. 1 dyrektywy NIS).

W przedmiotowej ustawie wskazano, iż będzie ona określać organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy, a także zakres oraz tryb stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej. W tym kontekście wątpliwości nie może więc budzić fakt, że w przedmiotowej regulacji kluczowym pojęciem jest to dotyczące cyberbezpieczeństwa, przez które rozumieć należy – jak to ujęto w art. 2 pkt 4 KrajSysCyberU – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność, autentyczność i dostępność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Ponadto w art. 5 ust. 1 na wzór tego obowiązującego na gruncie dyrektywy NIS dookreślono pojęcie operatora usługi kluczowej jako podmiotu, o którym mowa w załączniku nr 1 do ustawy, posiadającego jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

Usługę kluczową zdefiniowano natomiast jako usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych (art. 2 pkt 16 KrajSysCyberU).

Co istotne z punktu widzenia podjętej w niniejszym opracowania analizy, w załączniku nr 2 do KrajSysCyberU zdefiniowano także pojęcie usługi przetwarzania w chmurze, tj. jako usługi umożliwiającej dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników oraz – w art. 2 pkt 15 – usługi cyfrowej, tj. jako usługi świadczonej drogą elektroniczną w rozumieniu ustawy z 18.7.2002 r. o świadczeniu usług drogą elektroniczną[38] wymienioną w załączniku nr 2 KrajSysCyberU, a więc internetową platformą handlową, usługą przetwarzania w chmurze, wyszukiwarką internetową.

Odnosząc się jednak w pierwszej kolejności do podmiotów świadczących usługi w sektorze ochrony zdrowia, wskazać należy, iż w analizowanym tekście KrajSysCyberU jako operatorów usługi kluczowej należących do wspomnianego sektora wyodrębniono m.in.[39] podmiot leczniczy, o którym mowa w art. 4 ust. 1 DziałLeczU[40].

To więc na tych podmiotach leczniczych, wobec których właściwy organ wyda decyzję o uznaniu ich za operatów usług kluczowych, ciążyć będzie obowiązek spełnienia wielu wymogów określonych przepisami KrajSysCyberU, które sprowadzać będą się m.in. do:

1) prowadzenia systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem,
2) wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
   a) utrzymanie i bezpieczną eksploatację systemu informacyjnego,
   b) bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
   c) bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
   d) wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,

[37] Ponadto funkcjonuje dokument w postaci Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, który to jest krajową strategią w zakresie bezpieczeństwa systemów teleinformatycznych w rozumieniu Dyrektywy NIS, zob. Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, https://www.gov.pl/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022 (dostęp z 27.12.2017 r.).

[38] T.j. Dz. U. z 2017 r. poz. 1219 ze zm.

[39] Ponadto załącznik Nr 1 KrajSysCyberU obejmuje takie podmioty wchodzące w sektor ochrony zdrowia, jak: jednostka podległa ministrowi właściwemu do spraw zdrowia, właściwa w zakresie systemów informacyjnych ochrony zdrowia; Narodowy Fundusz Zdrowia, podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje dział farmacji szpitalnej w rozumieniu ustawy z 6.9.2001 r. – Prawo farmaceutyczne (t.j. Dz.U. z 2017 r. poz. 2211 ze zm.); podmiot leczniczy, w przedsiębiorstwie którego funkcjonuje apteka szpitalna w rozumieniu prawa farmaceutycznego; przedsiębiorca prowadzący działalność polegającą na prowadzeniu hurtowni farmaceutycznej w rozumieniu prawa farmaceutycznego; przedsiębiorca lub podmiot prowadzący działalność gospodarczą w państwie członkowskim UE lub państwie członkowskim Europejskiego Porozumienia o Wolnym Handlu (EFTA) – stronie umowy o Europejskim Obszarze Gospodarczym, który uzyskał pozwolenie na dopuszczenie do obrotu produktu leczniczego; importer produktu leczniczego/substancji czynnej w rozumieniu prawa farmaceutycznego; wytwórca produktu leczniczego/substancji czynnej w rozumieniu prawa farmaceutycznego; importer równoległy w rozumieniu prawa farmaceutycznego; dystrybutor substancji czynnej w rozumieniu prawa farmaceutycznego prowadzący działalność w formie apteki ogólnodostępnej w rozumieniu prawa farmaceutycznego.

[40] Tj.: 1) przedsiębiorcy w rozumieniu przepisów ustawy z 6.3.2018 r. – Prawo przedsiębiorców (t.j. Dz.U. z 2019 r. poz. 1292 ze zm.) we wszelkich formach przewidzianych dla wykonywania działalności gospodarczej, jeżeli ustawa nie stanowi inaczej, 2) samodzielne publiczne zakłady opieki zdrowotnej, 3) jednostki budżetowe, w tym państwowe jednostki budżetowe tworzone i nadzorowane przez Ministra Obrony Narodowej, ministra właściwego do spraw wewnętrznych, Ministra Sprawiedliwości lub Szefa Agencji Bezpieczeństwa Wewnętrznego, posiadające w strukturze organizacyjnej ambulatorium, ambulatorium z izbą chorych lub lekarza podstawowej opieki zdrowotnej, 4) pielęgniarkę podstawowej opieki zdrowotnej lub położną podstawowej opieki zdrowotnej w rozumieniu przepisów ustawy z 27.10.2017 r. o podstawowej opiece zdrowotnej (t.j. Dz.U. z 2020 r. poz. 172 ze zm.), 5) instytuty badawcze, o których mowa w art. 3 ustawy z 30.4.2010 r. o instytutach badawczych (t.j. Dz.U. z 2020 r. poz. 1383), 5a) fundacje i stowarzyszenia, których celem statutowym jest wykonywanie zadań w zakresie ochrony zdrowia i których statut dopuszcza prowadzenie działalności leczniczej, posiadające osobowość prawną jednostki organizacyjne stowarzyszeń, o których mowa w pkt 5, 6) osoby prawne i jednostki organizacyjne działające na podstawie przepisów o stosunku Państwa do Kościoła Katolickiego w Rzeczypospolitej Polskiej, o stosunku Państwa do innych kościołów i związków wyznaniowych oraz o gwarancjach wolności sumienia i wyznania, 7) jednostki wojskowe – w zakresie w jakim wykonują działalność leczniczą (art. 4 ust. 1 DziałLeczU).

e) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;
3) zbierania informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
4) zarządzania incydentami;
5) stosowania środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
   b) dbałość o aktualizację oprogramowania,
   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
6) stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa (art. 8 KrajSysCyberU).

W odniesieniu do dostawców usług cyfrowych ustawa o krajowym systemie cyberbezpieczeństwa zakłada, że również i oni będą odpowiedzialni za zapewnienie cyberbezpieczeństwa świadczonych przez nich usług[41]. I choć z całą pewnością na podstawie regulacji przedmiotowej ustawy obowiązki dla dostawców usług cyfrowych będą objęte łagodniejszym reżimem[42], niemniej jednak wskazać jeszcze należy, że ich działalność objęta będzie regulacją rozporządzenia wykonawczego Komisji Europejskiej (UE) 2018/151 z 30.1.2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącym ryzykiem dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ[43], i które to rozporządzenie precyzuje, jakie środki techniczne i organizacyjne powinien podjąć dostawca usług cyfrowych, aby zapewnić bezpieczeństwo systemów teleinformatycznych służących do świadczenia usług cyfrowych.

Z punktu widzenia omawianego tematu zasadniczą kwestią pozostaje jednak ustalenie, że mocą przepisów dyrektywy NIS i będącej jej implementacją KrajSysCyberU nałożonych zostanie wiele obowiązków i to zarówno na podmioty lecznicze działające w sektorze ochrony zdrowia (w tym również na te przetwarzające dokumentację medyczną na bazie technologii *cloud computing*), jak i samych dostawców usług chmury obliczeniowej (także tych świadczących usługi w sektorze ochrony zdrowia).

## Podsumowanie

Uwzględniając dotychczasowe ustalenia co do szerokiego zakresu obowiązków nałożonych na podmioty, które to przetwarzają dokumentację medyczną w postaci elektronicznej, zupełnie nie może dziwić fakt, iż znakomita większość świadczeniodawców, poradni podstawowej opieki zdrowotnej, gabinetów specjalistycznych, grupowych poradni lekarskich, pielęgniarskich czy rehabilitacyjnych, nie jest i nie będzie w stanie w najbliższej przyszłości sprostać tymże wymaganiom[44]. Stąd też dla części z nich remedium stanowić będzie bądź już obecnie stanowi właśnie technologia chmury obliczeniowej, niwelująca jednocześnie konieczność tworzenia i utrzymywania lokalnego ośrodka komputerowego, tworzenia specjalistycznych sieci transmisji danych czy zatrudniania wysoko wyspecjalizowanego personelu IT[45]. Z tego też względu wykorzystywanie usług podmiotów zewnętrznych, w szczególności dostawców usług *cloud computing*, przestało być w sektorze ochrony zdrowia nowością, a powoli staje się standardowym sposobem prowadzenia dokumentacji medycznej, czego doskonałym potwierdzeniem zdaje się być analiza rynku usług opieki zdrowotnej i możliwe do wskazania szerokie spektrum przykładów obejmujących współpracę zarówno na linii publicznej, jak i prywatnej opieki zdrowotnej z dostawcami usług medycznych.

W zakresie pierwszej z nich wskazać więc można zarówno na jednostkowe przykłady, tj. na współpracę, jaka

[41] W związku z tym zobowiązani będą oni m.in. podjąć właściwe i proporcjonalne środki techniczne i organizacyjne określone w rozporządzeniu wykonawczym 2018/151 w celu zarządzania ryzykiem, na jakie narażone są systemy informacyjne wykorzystywane do świadczenia usługi cyfrowej. Środki te zapewniają cyberbezpieczeństwo odpowiednie do istniejącego ryzyka oraz uwzględniają: 1) bezpieczeństwo systemów informacyjnych i obiektów; 2) postępowanie w przypadku obsługi incydentu; 3) zarządzanie ciągłością działania dostawcy w celu świadczenia usługi cyfrowej; 4) monitorowanie, audyt i testowanie; 5) najnowszy stan wiedzy, w tym zgodność z normami międzynarodowymi, o których mowa w rozporządzeniu wykonawczym 2018/151 (art. 17 ust. 2 KrajSysCyberU). Dostawca usługi cyfrowej podejmuje środki zapobiegające i minimalizujące wpływ incydentów na usługę cyfrową w celu zapewnienia ciągłości świadczenia tej usługi (art. 17 ust. 3 KrajSysCyberU). Ponadto ustawodawca nałożył na dostawców usług cyfrowych m.in. obowiązki związane z identyfikowaniem incydentów oraz ich zgłaszaniem (art. 18 ust. 1 KrajSysCyberU) do CSIRT NASK i in.

[42] Szerzej o zakresie obowiązków dostawców usług cyfrowych na gruncie przepisów ustawy o krajowym systemie cyberbezpieczeństwa w rozdziale 4 KrajSysCyberU.

[43] Dz.Urz. UE L Nr 26, s. 48.

[44] *A. Romaszewski*, *W. Trąbka*, *M. Kielar*, *K. Gajda*, Elektroniczna dokumentacja medyczna – przetwarzanie danych o stanie zdrowia poza miejscem świadczenia usług zdrowotnych..., s. 16.

[45] Podkreślenia wymaga fakt, że implementacja elektronicznej dokumentacji medycznej, w tym także tej opartej na technologii *cloud computing*, przynosi nie tylko potencjalne zagrożenia i konieczność sprostania wielu wymaganiom, ale też niesie z sobą wiele korzyści, i to dla wielu uczestników ochrony zdrowia: tj. pacjentów, personelu medycznego, menadżerów placówek zdrowia, płatnika, a także całego systemu ochrony zdrowia. Zob. *D.M Szymczyk*, *A. Horoch*, Implementacja elektronicznej dokumentacji medycznej. Część 2 – korzyści dla uczestników systemu ochrony zdrowia, Medycyna Ogólna i Nauki o Zdrowiu, 2013, t. 19, Nr 3, s. 324–330.

nastąpiła do 2014 r. na linii między ePUAP[46] a Comarch, czy na współpracę na linii między Szpitalem Klinicznym Przemienienia Pańskiego Uniwersytetu Medycznego w Poznaniu a firmą Rightsoft Sp. z o.o.[47], jak też szerzej na przykłady dotyczące regionalnych projektów zrealizowanych w zakresie e-zdrowia w poszczególnych województwach[48].

Powszechnym zjawiskiem jest również korzystanie z podmiotów prywatnych oferujących opiekę zdrowotną z technologii chmury obliczeniowej udostępnianej chociażby przez takich dostawców, jak np. Microsoft[49].

[46] ePUAP, czyli Elektroniczna Platforma Usług Administracji Publicznej, to ogólnopolska platforma teleinformatyczna służąca do komunikacji obywateli z jednostkami administracji publicznej w ujednolicony, standardowy sposób. Umożliwia ona także komunikację między sobą podmiotom administracji publicznej. Po raz pierwszy ePUAP uruchomiony został 14.4.2008 r., natomiast 17.8.2015 r. został uruchomiony tzw. EPUAP2. Zarządzaniem platformą zajmuje się obecnie Centrum Projektów Informatycznych (CPI), https://www.gov.pl/cyfryzacja/serwis-epuap (dostęp z 17.12.2017 r.).

[47] Rightsoft Sp. z o.o. 28.9.2015 r. podpisała umowę ze Szpitalem Klinicznym Przemienienia Pańskiego UM w Poznaniu, na mocy której rozpoczęła wdrożenie Elektronicznej Dokumentacji Medycznej, https://www.system-eskulap.pl/wdrozenie-elektronicznej-dokumentacji-medycznej/ (dostęp z 19.12.2017 r.).

[48] Szerzej zob. *G. Fiuk*, Doświadczenia z realizacji regionalnych projektów e-zdrowie w Polsce – wyzwania, bariery, problemy, korzyści i rekomendacje, [w:] *K. Flaga-Gieruszyńska*, *J. Gołaczyński*, *D. Szostek* (red.), E-obywatel, E-sprawiedliwość, E-usługi, Warszawa 2017, s. 57–66.

[49] Zob. więcej Microsoft, Nowe możliwości w ochronie zdrowia, *www.houseofcloud.pl/wp-content/uploads/2017/.../Raport-Microsoft-dla-Zdrowia.pdf* (dostęp z 19.12.2017 r.).

**Słowa kluczowe:** *cloud computing*, dane osobowe, dane dotyczące zdrowia, elektroniczna dokumentacja medyczna, RODO, dyrektywa NIS.

## Legal aspects of using cloud computing technology in the area of healthcare

*The purpose of the present article is an attempt to answer the question regarding legal implications of using cloud computing technology in the area of healthcare, specifically the possibility to process data regarding health within electronic medical record which is present in such information systems as cloud computing. Therefore, the main background of deliberations are regulations of the European Parliament and the Council of 27 April 2016, on protection of natural persons in regard to processing of personal data and free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), and also – on a smaller scale – regulations of Directive of the European Parliament and the Council 2016/1148 of 6 July 2016, regarding resources for a high and common level of security of the Web and information systems within the EU, and regulations of Polish law amended on that basis.*

**Keywords:** cloud computing, personal data, health data, electronic health record, GDPR, Network and Information Systems Directive.